FortiSIEM®

Unified event correlation and risk management for modern networks

Security is no longer just about protecting information, it is critical to maintaining trust with customers and protecting the organization's brand and reputation.

Security and Compliance Made Easy

Breaches cause customers to take their business elsewhere, resulting in material and substantially negative impacts to an organization's bottom line. Attracting new customers is estimated at seven times more costly than keeping existing customers. Fines and legal fees can quickly add up. Publicly traded organizations can see negative and lasting impacts to their stock value, supplier relationships and shareholder perceptions. All these add up to explain why more boards are getting involved in security decisions. FortiSIEM provides organizations with a comprehensive, holistic and scalable solution, from IoT to the Cloud, with patented analytics that are actionable to tightly manage network security, performance and compliance standards, all delivered through a single pane of glass view of the organization.

Unified NOC and SOC Analytics (Patented)

Fortinet has developed an architecture that enables unified and cross-correlated analytics from diverse information sources including logs, performance metrics, SNMP Traps, security alerts and configuration changes. FortiSIEM essentially takes the analytics traditionally monitored in separate silos from — SOC and NOC — and brings that data together for a more holistic view of the threat data available in the organization. Every piece of information is converted into an event which is first parsed and then fed into an event-based analytics engine for handling real-time searches, rules, dashboards and ad-hoc queries.

Highlights

- Unified, Real-Time, Network Analytics
- Single IT Pane of Glass
- Multi-tenancy
- MSP/MSSP Ready
- Cross Correlation of SOC & NOC Analytics
- Self Learning Asset Inventory
- Cloud Scale Architecture
- Security and Compliance out-of-the-box

HIGHLIGHTS

External Threat Intelligence (TI) feeds from open source threat intelligence feeds, commercial sources and custom data sources integrate easily into the FortiSIEM TI framework. This grand unification of diverse sources of data enables organizations to quickly create comprehensive dashboards and reports to more rapidly identify root causes of threats, and take the steps necessary to remediate and prevent them in the future.

Distributed Real-Time Event Correlation (Patented)

Distributed event correlation is a difficult problem, as multiple nodes have to share their partial states in real-time to trigger a rule. While many SIEM vendors have distributed data collection and distributed search capabilities, Fortinet is the only vendor with a distributed real-time event correlation engine. Complex event patterns in real-time can be detected with minimal delay. This patented algorithm enables FortiSIEM to handle a large number of rules in real-time at high event rates for greatly increased detection timeframes.

Real-Time, Automated Infrastructure Discovery and Application Discovery Engine (CMDB)

Rapid problem resolution requires infrastructure context. Most log analysis and SIEM vendors require administrators to provide the context manually, which quickly becomes stale, and is highly prone to human error. Fortinet has developed an intelligent infrastructure and application discovery engine that is able to discover and map the topology of both physical and virtual infrastructure, on-premises and in public/private clouds simply using credentials without any prior knowledge of what the devices or application is.

Discovery is both wide (covering a large number of Tier 1/2/3 vendors) and deep (covering system, hardware, software, running services, applications, storage, users, network configuration, topology and device relationships). Discovery can run on-demand or on schedule to detect (in real-time) infrastructure changes and report on any new devices and applications detected — this is an essential part of compliance requirement management that FortiSIEM is uniquely able to meet. An up-to-date (Centralized Management Database) CMDB enables sophisticated context aware event analytics using CMDB Objects in search conditions.

Dynamic User Identity Mapping

Crucial context for log analysis is connecting network identity (IP address, MAC Address) to user identity (log name, full name, organization role). This information is constantly changing as users obtain new addresses via DHCP or VPN.

Fortinet has developed a dynamic user identity mapping methodology. First, users and their roles are discovered from on-premises repositories such as Microsoft Active Directory and Open LDAP, or from Cloud SSO repositories such as OKTA. This can be run on-demand or on a schedule to detect new users. Simultaneously, network identity is identified from important network events such as firewall network translation events, Active Directory logons, VPN logons, WLAN logons, Host Agent registration logs, etc. Finally, by combining user identity, network identity and geo-identity in a real-time distributed in-memory database, FortiSIEM is able to form a dynamic user identity audit trail. This makes it possible to create policies or perform investigations based on user identity instead of IP addresses — allowing for rapid problem resolution.

Flexible and Fast Custom Log Parsing Framework (Patented)

Effective log parsing requires custom scripts but those can be slow to execute, especially for high volume logs like Active Directory, firewall logs, etc. Compiled code on the other hand, is fast to execute but is not flexible since it needs new releases. Fortinet has developed an XML-based event parsing language that is functional like high level programming languages and easy to modify yet can be compiled during run-time to be highly efficient. All FortiSIEM parsers go beyond most competitor's offerings using this patented solution and can be parsed at beyond 10K EPS per node.

Hybrid Database Architecture — Leveraging Structured and Unstructured Data Feeds

FortiSIEM takes advantage of two diverse sources of information — discovered information is structured data suitable for a traditional relational database, while logs, performance metrics etc. are unstructured data which needs a NoSQL-type database. Fortinet has developed a hybrid approach where the data is stored in optimized databases with unique business layer logic providing a comprehensive, single database abstraction layer.

The user is able to search for events (stored in NoSQL database) using CMDB objects (stored in relational database). This approach harnesses the power and benefits of both databases.

HIGHLIGHTS

Large Scale Threat Feed Integration

There are many sources available for customers to subscribe to external threat feeds in managing potential threats in their network. However, threat feed information can be very large, often reaching millions of IP addresses, malware domains, hashes and URLs, and the information can also quickly become stale as malware websites and domain are taken down and brought up. This provides a significant computational challenge to the consumers of threat intelligence data. Fortinet has developed proprietary algorithms that enable this large amount of information to be quickly obtained from the source, then effectively distributed to various FortiSIEM nodes and evaluated in real-time at higher rates than other providers (exceeding 10K EPS per node).

Large Enterprise and Managed Service Provider Ready — "Multi-Tenant Architecture"

Fortinet has developed a highly customizable, multi-tenant architecture that enables enterprises and service providers to manage a large number of physical/logical domains and over-lapping systems and networks from a single console. In this environment it is very easy to cross-correlate information across physical and logical domains, and individual customer networks. Unique reports, rules and dashboards can easily be built for each, with the ability to deploy them across a wide set of reporting domains, and customers. Event archiving policies can also be deployed on a per domain or customer basis.

FEATURES

Real-Time Operational Context for Rapid Security Analytics

- Continually updated and accurate device context — configuration, installed software and patches, running services
- System and application performance analytics along with contextual inter-relationship data for rapid triaging of security issues
- User context, in real-time, with audit trails of IP addresses, user identity changes, physical and geo-mapped location data context
- Detect unauthorized network devices and applications, configuration changes

Out-of-the-Box Compliance Reports

- Out-of-the-box pre-defined reports supporting a wide range of compliance auditing and management needs including — PCI-DSS, HIPAA, SOX, NERC, FISMA, ISO, GLBA, GPG13, SANS Critical Controls

Performance Monitoring

- Monitor basic system/common metrics
- System level via SNMP, WMI, PowerShell
- Application level via JMX, WMI, PowerShell
- Virtualization monitoring for VMware, HyperV — guest, host, resource pool and cluster level
- Storage usage, performance monitoring — EMC, NetApp, Isilon, Nutanix, Nimble, Data Domain
- Specialized application performance monitoring
- Microsoft Active Directory and Exchange via WMI and Powershell
- Databases — Oracle, MS SQL, MySQL via JDBC
- VoIP infrastructure via IPSLA, SNMP, CDR/CMR
- Flow analysis and application performance — Netflow, SFlow, Cisco AVC, NBAR
- Ability to add custom metrics
- Baseline metrics and detect significant deviations

Real-Time Configuration Change Monitoring

- Collect network configuration files, stored in a versioned repository
- Collect installed software versions, stored it in a versioned repository
- Automated detection of changes in network configuration and installed software
- Automated detection of file/folder changes — Windows and Linux — who and what details
- Automated detection of changes from an approved configuration file
- Automated detection of windows registry changes via FortiSIEM windows agent

FEATURES

Device and Application Context

- Network Devices including Switches, Routers, Wireless LAN
- Security devices — Firewalls, Network IPS, Web/Email Gateways, Malware Protection, Vulnerability Scanners
- Servers including Windows, Linux, AIX, HP UX
- Infrastructure Services including DNS, DHCP, DFS, AAA, Domain Controllers, VoIP
- User-facing Applications including Web Servers, App Servers, Mail, Databases
- Storage devices including NetApp, EMC, Isilon, Nutanix, Data Domain
- Cloud Apps including AWS, Box.com, Okta, Salesforce.com
- Cloud infrastructure including AWS
- Environmental devices including UPS, HVAC, Device Hardware
- Virtualization infrastructure including VMware ESX, Microsoft HyperVScalable and Flexible Log Collection

Scalable and Flexible Log Collection

- Collect, Parse, Normalize, Index and Store security logs at very high speeds (beyond 10K events/sec per node)
- Out-of-the-box support for a wide variety of security systems and vendor APIs — both on-premises and cloud
- Windows Agents provide highly scalable and rich event collection including file integrity monitoring, installed software changes and registry change monitoring
- Linux Agents for file integrity monitoring
- Modify parsers from within the GUI and redeploy on a running system without downtime and event loss
- Create new parsers (XML templates) via integrated parser development environment and share among users via export/import function
- Securely and reliably collect events for users and devices located anywhere

Notification and Incident Management

- Policy-based incident notification framework
- Ability to trigger a remediation script when a specified incident occurs
- API-based integration to external ticketing systems — ServiceNow, ConnectWise, and Remedy
- Built-in ticketing system

Rich Customizable Dashboards

- Configurable real-time dashboards, with “Slide-Show” scrolling for showcasing KPIs
- Sharable reports and analytics across organizations and users
- Color-coded for rapidly identifying critical issues
- Fast — updated via in-memory computation
- Specialized layered dashboards for business services, virtualized infrastructure, and specialized apps

External Threat Intelligence Integrations

- API’s for integrating external threat feed intelligence — Malware domains, IPs, URLs, hashes, Tor nodes
- Built-in integration for popular threat intelligence sources — ThreatStream, CyberArk, SANS, Zeus
- Technology for handling large threat feeds — incremental download and sharing within cluster, real-time pattern matching with network traffic

Powerful and Scalable Analytics

- Search events in real — without the need for indexing
- Keyword-based searches & searches by parsed event attributes
- Search historical events — SQL-like queries with Boolean filter conditions, group by relevant aggregations, time-of-day filters, regular expression matches, calculated expressions — GUI & API
- Trigger on complex event patterns in real-time
- Use discovered CMDB objects and user/identity and location data in searches and rules
- Schedule reports and deliver results via email to key stakeholders
- Search events across the entire organization, or down to a physical or logical reporting domain
- Dynamic watch lists for keeping track of critical violators — with the ability to use watch lists in any reporting rule
- Scale analytics feeds by adding Worker nodes without downtime
- Incident reporting prioritization can be implemented via critical Business Service

Base-lining and Statistical Anomaly Detection

- Baseline endpoint/server/user behavior — hour of day and weekday/weekend granularity
- Highly flexible — any set of keys and metrics can be “baselined”
- Built-in and Customizable triggers on statistical anomalies

External Technology Integrations

- Integration with any external web site for IP address lookup
- API-based integration for external threat feed intelligence sources
- API-based 2-way integration with help desk systems — seamless, out-of-the box support for ServiceNow, ConnectWise and Remedy
- API-based 2-way integration with external CMDB — out-of-the box support for ServiceNow and ConnectWise
- Kafka support for integration with enhanced Analytics Reporting — i.e. ELK, Tableau and Hadoop
- API for easy integration with provisioning systems
- API for adding organizations, creating credentials, triggering discovery, modifying monitoring events

FEATURES

Simple and Flexible Administration

- Web-based GUI
- Rich Role-based Access Control for restricting access to GUI and data at various levels
- All inter-module communication protected by HTTPS
- Full audit trail of FortiSIEM user activity
- Easy software upgrade with minimal downtime & event loss
- Easy way to update FortiSIEM knowledge base updates (parsers, rules, reports)
- Policy-based archiving
- Hashing of logs at time for non-repudiation & integrity verification
- Flexible user authentication — local, external via Microsoft AD and OpenLDAP, Cloud SSO/SAML via Okta
- Ability to log into remote server behind a collector from FortiSIEM GUI via remote SSH tunnel

Easily Scale Out Virtualized Architecture

- Available as Virtual Machines for on-premises and public/private cloud deployments on the following hypervisors — VMware ESX, Microsoft HyperV, KVM, Xen, Amazon Web Services AMI, OpenStack, Azure
- Scale data collection by deploying Collector virtual machines
- Collectors can buffer events when connection to FortiSIEM cloud is not available
- Scale analytics by deploying Worker virtual machines
- Built-in load balanced architecture for collecting events from remote sites via collectors

Threat Intelligence Center via Beaconing

- FortiSIEM instances send health and anonymized incidents to FortiSIEM Cloud
- Cross-correlation across multiple FortiSIEM instances identifies emerging trends and developing malware in the wild

Availability Monitoring

- System up/down monitoring — via Ping, SNMP, WMI, Uptime Analysis, Critical Interface, Critical Process and Service, BGP/OSPF/EIGRP status change, Storage port up/down
- Service availability modeling via Synthetic Transaction Monitoring — Ping, HTTP, HTTPS, DNS, LDAP, SSH, SMTP, IMAP, POP, FTP, JDBC, ICMP, trace route and for generic TCP/UDP ports
- Hardware and environmental monitoring
- Maintenance calendar for scheduling maintenance windows
- SLA calculation — “normal” business hours and after-hours considerations

SPECIFICATIONS

FortiSIEM Windows Agents

Fortinet has developed a highly efficient agentless technology for collecting information. However some information such as file integrity monitoring data is expensive to collect remotely. FortiSIEM has combined its agentless technology with newly developed high performance agents to significantly bolster its data collection.

	AGENTLESS TECHNOLOGY	BASIC AGENT	ADVANCED AGENT
Agentless			
Discovery	•		
Performance Monitoring	•		
(Low Performance) Collect System, App & Security Logs	•		
Agents			
(High Performance) Collect System, App & Security Logs		•	•
Collect DNS, DHCP, DFS, IIS Logs		•	•
Up to 1800 events/second/server loss less, low latency		•	•

	AGENTLESS TECHNOLOGY	BASIC AGENT	ADVANCED AGENT
Up to 500 Agents per Agent Manager		•	•
Local Parsing and Time Normalization		•	•
Installed Software Detection			•
Registry Change Monitoring			•
File Integrity Monitoring			•
Customer Log File Monitoring			•
WMI Command Output Monitoring			•
PowerShell Command Output Monitoring			•

ORDER INFORMATION

Licensing Scheme

FortiSIEM licenses provide the core functionality for network device discovery. Devices include switches, routers, firewalls, servers, etc. Each device that is to be monitored requires a license. Each license supports data capture and correlation, alerting and alarming, reports, analytics, search and optimized data repository and includes 10 EPS (Events Per Second). “EPS” is a performance measurement that defines how many messages or events are generated by each device in a second. Additional EPS can be purchased separately as needed. Licenses are available in either a “Subscription” or “Perpetual” version.

PRODUCT	SKU	DESCRIPTION
FortiSIEM Base Product		
FortiSIEM All-In-One Perpetual License	FSM-AIO-BASE	Base all-in-one Perpetual License for 50 devices and 500 EPS
	FSM-AIO-XX-UG	Add XX devices and EPS/device all-in-one Perpetual License for Non-MSP/MSSPs
FortiSIEM All-In-One Perpetual License	FC[1-8]-10-FSM98-180-02-DD	Per Device Subscription License that manages minimum XX devices, 10 EPS/device
FortiSIEM Additional Products		
FortiSIEM End-Point Device Perpetual License	FSM-EPD-XX-UG	Add XX End-Points and 2 EPS/End-Point for all-in-one Perpetual License
FortiSIEM End-Point Device Subscription License	FC[1-8]-10-FSM98-184-02-DD	Per End-Point Subscription License for minimum XX End-Points, 2 EPS/End-Point
Add 1 EPS Perpetual License	FSM-EPS-100-UG	Add 1 EPS Perpetual
Add 1 EPS Subscription License	FC[1-10]-FSM98-183-02-DD	Add 1 EPS Subscription
FortiSIEM Basic Windows Agent Perpetual License	FSM-WIN-XX-UG	XX Basic Windows Agents for Perpetual License
FortiSIEM Advanced Windows Agent Perpetual License	FSM-WIN-ADV-XX-UG	XX Advanced Windows Agents for Perpetual License
FortiSIEM Basic Windows Agent Subscription License	FC[1-8]-10-FSM98-181-02-DD	Per Agent Subscription License for minimum XX Basic Windows Agents
FortiSIEM Advanced Windows Agent Subscription License	FC[1-8]-10-FSM98-182-02-DD	Per Agent Subscription License for minimum XX Advanced Windows Agents
IOC Service Subscription License	FC[1-G]-10-FSM98-149-02-DD	(X Points) FortiSIEM Indicators of Compromise (IOC) Service. 1 device or 2 End-Points or 3 Windows Agents equals 1 point.
FortiSIEM Support		
FortiCare Support for FortiSIEM	FC[1-G]-10-FSM97-248-02-DD	24x7 FortiCare Contract (X Points). 1 device or 2 End-Points or 3 Windows Agents equals 1 point.

GLOBAL HEADQUARTERS
Fortinet Inc.
899 KIFER ROAD
Sunnyvale, CA 94086
United States
Tel: +1.408.235.7700
www.fortinet.com/sales

EMEA SALES OFFICE
905 rue Albert Einstein
06560 Valbonne
France
Tel: +33.4.8987.0500

APAC SALES OFFICE
300 Beach Road 20-01
The Concourse
Singapore 199555
Tel: +65.6395.2788

LATIN AMERICA SALES OFFICE
Sawgrass Lakes Center
13450 W. Sunrise Blvd., Suite 430
Sunrise, FL 33323
United States
Tel: +1.954.368.9990